



DİJİTAL AKTİVİZMİN BİR TÜRÜ OLARAK HACKTİVİZM VE “RedHack”

HACKTIVISM AND “RedHack” AS A SORT OF DIGITAL ACTIVISM

Arş. Gör. Ceren Yegen ¹

Muş Alparslan Üniversitesi, İletişim Fakültesi,
Gazetecilik Bölümü,
Muş

Özet: Özellikle 21.yüzyılda hızla gelişen iletişim teknolojileri, iletişim olgusunun kendi içerisinde değişip dönüşmesine sebep olurken, toplumsal gündelik yaşam pratiklerinin de değişip dönüşmesine neden olmaktadır. İletişim teknolojileri ile yerel olandan küresel olana doğru bir dönüşüm seyretmekle birlikte, bu durum birçok alanı da etkilemektedir. İletişim ve internet teknolojilerinin gelişim ve dönüşümü ile beraber birçok toplumsal pratik sosyal mecralardan dijital mecralara taşınmaktadır. Bireyler bireysel ya da toplumsal birçok pratiği iletişim ve internet teknolojilerinden yararlanarak dijital ortamlarda yapmakta, bu sayede daha fazla kitleye, daha kısa sürede ulaşabilmektedir. Böylelikle ayrıca geleneksel iletişimin tek yönlü duruşuna artık etkileşimden söz eden ve çift yönlü işleyen bir iletişim ortam ile algısı noktasında bir alternatif getirilmektedir. Bununla birlikte örgütlenme pratiği de büyük bir önem kazanmış ve insanlar internet üzerinden daha çabuk ve etkili şekilde örgütlenebilir olmuştur. Bu anlamda önemli bir toplumsal pratik olan aktivizm de internet teknolojileri ile dönüşmüş ve aktivizmin internet üzerinden yapılmasını ifade eden dijital aktivizm önemli bir kavram olarak ortaya çıkmıştır. Bu yüzden bu çalışmada sınırlı kalmak adına bir dijital aktivizm pratiği olan ve özellikle Türkiye’de 1997 yılında kurulan ve Kızıl Hackerlar Birliği olarak anılan "RedHack" isimli hacker grubu ile öne çıktığı varsayılan "hacktivizm" kavramı RedHack’in 2012 ile 2013 arasında yaptığı eylemler (toplam 33 eylem) çerçevesinde tartışılacak, politik gerekçeler ile hackleme eylemi yapma anlamına gelen hacktivizm kavramının yeni medya destekli olarak nasıl yorumlandığı betimsel bir analiz dahilinde irdelenecektir.

Anahtar Sözcükler: İletişim Teknolojileri, İnternet, Aktivizm, Dijital Aktivizm, Hacktivizm, RedHack.

Extended Abstract: The change is observed with phenomenon of globalization nearly for thirty years, have affected communication technologies, too. New world order is emerged parallel to neo-liberal policies modulated the phenomenon of communication which is an important organizer of social practices. It also gave consequence to phenomenon of communication and his rituals. Over the years like phenomenon of communication which contains nearly all daily life practices, communication technologies have changed, too. Communication technologies also have had big changes. These changes are about the media’s structural alterations and conversions. Media have changed and lived a lof of big alterations and conversions because of developing and changing communication technologies, global policies and customizings. It were also varied and had some structural rotations. With these alterations, conversions and rotations a “new media” and his practices are emerged. This kind of media which is new caused social and cultural changes and tendencies with his contents and implementations. All over the world both people and media hirers, media managers kept up

¹c.yegen@alparslan.edu.tr

with these alterations and conversions, and they also assumed these alterations as novelties. New media is described as traditional media's diverseness state that new world is changed with communication technologies and the new form of communication.

As the media communication technologies which are developed in 21st Century both lead to that phenomenon of communication transform and the social life's rituals' change/transform, too. A transformation is from local to global occurred with communication technologies and this situation affected a lot of channels. With the change and transformation of communication technologies', a lot of practice of individuals moved to digital areas from social areas. The individuals began to making their social or personal practices in digital areas thanks to communication technologies. Herewith the communication technologies more quickly reached to crowds.

New media is formed by new communication technologies procured a new, fast, interactive and multifaceted communication system as distinct from the traditional media. New media also caused digital areas which are public areas as part of discussion and reconciliation. In this manner traditional public areas replaced with digital areas in connection with public discussions and negotiations. Thanks to the internet which is one of new media technologies' result people began to pay their bills via the internet, find their friends or relatives make their banking operations. Like their daily rituals, individuals began to make their socialization practices via the internet and his social areas. The individuals share their photographs, videos or status update by way of social networking sites like Facebook or Twitter. Hereby while they are socialising, they also formalize the human relations online editing, too. The online platforms like blogs, social networking sites and the websites formalized both the flow of information and the phenomenon of socialization and communication action. The information is earned from traditional media have disseminated a diversity. Herewith the information are expanded to everywhere more quickly and easily. This situation as an advantage made people important. Hereby an individual became both the information's supplier and owner. In addition the unidirectional flow of information in traditional media is refracted. Alternative media organs, the citizen journalism or online journalism are some examples of new and individual-oriented media executions. Thanks to new media practices with these applications, the individuals began to produce their own news and he began to interfere the news contents, too. Media's these changes and transformations caused to interrogate the media's future and the professionalism of occupation. Although these interrogation being reporter, media worker or journalist made people good and these applications caused a lot of digital novelties, too. Hereby also an alternative which provide an interactive communication period as part of a bivious communication occurred against to the perception that the traditional communication is one way. Also the practice of organizing became important and people are organized via the internet more quickly and effective. In this sense activism which is an important social practice transformed and changed with communication technologies and digital activism which means that making activism on the internet occurred as an important concept.

"Digital activism" which states that making activist practices with communication technologies does not only an online practice. Digital activism braces up communication technologies and the internet enabled to making activist practices on online platforms or on the computer instead of main streets and avenues. A person who does not go to the streets for an activist action may join a digital activist action via the internet and he/she may be a part of an action. By this means people does not go to the streets for an activist action feel satisfied like they have gone to an activist action. These people may think that they carried through their citizenship care. Thus digital activism is also important as part of consciousness of citizenship. "Slacktivism" and "clicktivism" are the most important examples of digital activism today. Slacktivism which can be defined as the playing role to support an activist action via the internet and it is also called that "so-called" activism. Dissimilarly slacktivism, clicktivism refers to promoting a cause using social media and other online methods. Infact the concept of clicktivism procure the slacktivism. People support a digital action via the internet with a

"click" thanks to clicktivism and being a slacktivist a person may share clicktivist applications by way of social networking sites. Hereby people both join digital actions and become aware of latest news. To support a digital action on computer namely slacktivism shines out in Turkey some online signature platforms like www.change.org, imza.la and www.avaaz.org etc. (These sites organize petitions on the internet.) and some donation platforms like LÖSEV, İHH, TEMA etc. Slacktivism is a crowdsourced (a concept is derived from crowd and outsourcing refers the concept of crowdsource) system ensure to support a social event or action and it enable to use crowdsources. Hereby slacktivism reaches extensive areas, crowds and provide to participating digital actions where you are. Slacktivism or clicktivism also do not impose any limitation or possessive to join a petition or donation campaign.

No doubt hacktivism is one of the most important kind of digital activism. Hacktivism refers to hacking action because of politic reasons. Hacktivism purpose to warning politic channels in connection with some social events, cases. Hacktivism had a reputation for some hacktivist platforms like "Anonymous", "Cyber-Warriors", "LulzSEC" and "The Jester" in the world. In Turkey hacktivism had a reputation thanks to "RedHack." Hacktivism is both a new concept and new practice technics for Turkey. Although it is a new concept, it is famous for RedHack. In recent years RedHack and his actions are made with political reasons have come to the forefront in Turkey. RedHack became very popular in Turkey his actions are made with political reasons and hereby it is described as a hacktivist occurrence. In previous years "MANYAK" who is the leader of RedHack made a statement for Radikal Newspaper about their identities and place where they live. He has stated that they live in Turkey and do not have a connection with any organization. He has also stated that there are many people in RedHack like Alevists, Kemalists, Atheist, Kurds and Muslims.

RedHack's actions which have politic reasons generally are about governmental institution. These actions are made in Turkey have faced some legal executions. For example in March 21, 2012 specially authorized prosecutor had operations in some cities and a lot of people were taken into custody. Some of those (7 out of 17) were taken into custody on the grounds that they are member of Redhack, but after that an explanation was made which claims that these people do not have a connection with RedHack. In this sense in Turkey the politics of cyber security was formed by some laws since 2008. With these laws the Turkish Government have aimed to prevent cyber crimes.

As it is seen hacktivism is a new concept which is came up with the communication technologies and it is became famous with RedHack in Turkey. This situation showed that the concept of hacktivism sholud be examined. Thus in this study the concept of hacktivism which is a digital activism practice and in Turkey shined out with the group "RedHack" which was established in 1997, means "Union of Scarlet Hackers" were discussed with RedHack's actions (total 33 actions) which were made in 2012 and 2013 years, hacktivism which means that action of hacking under colour of politic were examined and how the concept of hacktivism is interpreted via the new media were discussed with a descriptive analysis.

It seems that RedHack which is examined in this study with his actions (total 33 actions) is a hacktivist occurrence and he targets generally the government policies with his cyber attacks for public welfare. He also assert that having information is a right of citizenship. Otherwise RedHack's actions were examined in this study are his efforts to point out some social events or problems. Although RedHack's actions did not engender radical changes, they taken attention to some social problems, expectations and wishes and they were also warnings for government agencies. Hereby we can easily say that RedHack did not overlook social problems, expectations or events.

We should also say that Turkey's cyber security policies which have a recent past should be examined with a wide range of communication technologies because, the phenomenon of the internet always finds out

new things, applications and technologies etc. We realised that in this study, RedHack and his actions were about social problems like the problem of milk distribution to schools in Turkey (in 2012 children were poisoned after the milk distribution in Turkey) or the government's practice of censor to some corporations or foundations etc. RedHack hacked some government foundations' websites and some milk company's websites as part of his reaction. RedHack's these actions were warnings for these foundations and companies. In this regard we can easily say that RedHack makes cyber actions as part of social problems or events for equality, justice and freedom.

Key Words: *Communication Technologies, The Internet, Activism, Digital Activism, Hacktivism, RedHack*

Giriş

Dijital aktivizm kavramı bugün aslında yeni iletişim teknolojilerinin içtimai bir sonucu olarak ortadadır. Aktivizmin iletişim teknolojilerini kullanarak dijital mecralarda icra edilmesi anlamına gelen dijital aktivizm; slaktivizm, kliktivizm, hacktivizm vb. türler ile kendisini göstermekte ve bireyleri yeni iletişim teknolojilerini kullanarak söz konusu aktivist faaliyetleri çok hızlı, etkili, çoksesli, eşzamanlı ve her yere ulaşabilir şekilde gerçekleştirmektedir. Politik gerekçeler görerek ya da göstererek hacking eylemi yapmak olarak tanımlanan hacktivizm de internet aracılığı ile yine internet üzerinden yapıldığından bu anlamda bir dijital aktivizm faaliyeti olarak gerçekleşmekte, dünyada Anonymous, Cyber-Warriors, LulzSEC vb. oluşumlar ile Türkiye'de ise RedHack isimli oluşum ile öne çıkmaktadır. İletişim teknolojilerinden aldığı güç ile adından son yıllarda sıkça söz ettiren hacktivizm Türkiye'de RedHack'in eylemleri vasıtası ile birçok içtimai soruna dikkat çekmiş ve genellikle devlet kurumlarını hedef almıştır. RedHack'in eylemleri, kökten toplumsal dönüşümlere sebep olmasa da toplumsal anlamda bir farkındalık yaratmayı başarmış ya da toplumun sorun diye adlettiği olayların gündemden düşmemesini sağlayarak söz konusu olaylara dikkat çekmiştir. Örneğin Redhack Gezi protestoları sürecinde Ankara'da başından vurularak öldürülen Ethem Sarısülük'ün ölümünü protesto etmek için Haziran 2013'te Ankara Emniyet Müdürlüğü ve İstanbul Valiliği internet sitelerini çökertmiştir. Bu anlamda yaptıkları açıklamada; "Ethem Sarısülük'ü başından vurarak katleden cemaatin yeşil ordu Ankara Polis'ini protesto ediyoruz!"² diyen RedHack o dönem toplumda büyük bir infial uyandıran Sarısülük olayına duyarsız kalmamıştır.

Bu yüzden bu çalışmanın konusu bir dijital aktivizm türü olarak hacktivizm kavramını RedHack örneği dahilinde tartışmaktır. Çalışmada RedHack'inhacktivist faaliyetlerinin betimsel bir analiz ile anlaşılması amaçlanmaktadır. Çalışmanın kapsam ve sınırlılığını RedHack ve RedHack'in 2012 - 2013 yılları arasında yaptığı eylemler oluşturmaktadır. Bu kapsam çerçevesinde Redhack'in 2012-2013 yılları arasında gerçekleştirdiği 33 eylem incelenmiştir. Çalışmada tek bir hacktivist oluşumun seçilmesinin sebebi RedHack'in Türkiye'de hacktivizm denince akla gelen ilk ve tek oluşum olmasıdır. Bu yüzden bu çalışmada RedHack'in hacktivizm bağlamında örneklem olarak alınması uygun görülmüştür. Kuramsal çerçevesini yeni medya ve dijital aktivizm tartışmalarının oluşturduğu bu çalışma kapsamında öncelikle yeni medya ve internet temelinde dijital aktivizm tartışılmış, hacktivizm kavramı ayrıntılı olarak ele alınmış, ardından RedHack'in Türkiye'de yaptığı hacktivist eylemler incelenmiş ve Türkiye'nin siber güvenlik noktasındaki durumu ile düzenlemelerinden bahsedilmiştir. Bu çalışma dijital aktivizm kavramının yeni medya destekli olarak nasıl okunduğunun anlaşılması açısından bir hayli önemlidir. Ayrıca çalışma, yeni iletişim teknolojileri sayesinde ortaya çıkan ve adından özellikle sosyal medya ekseninde söz ettirmeye başlayan dijital aktivizm ve türlerinin toplumsal pratikleri dijital ortam ve pratikler aracılığı ile nasıl dönüştürdüğüünün anlaşılmasına katkı sağlayacak niteliktedir.

² <http://www.sendika.org/2013/06/redhackten-ethem-sarisuluk-icin-eylem/>, 01.11.2014.

1. Dijital Aktivizm

Aktivizm pratiğinin dijital mecralarda iletişim teknolojileri aracılığı ile yapılmasını ifade eden dijital aktivizm günümüzün yeni ve popüler kavramlarından biridir. İletişim teknolojileri ve internetin 1980'lerden bu yana küresel bir çizgide hızla gelişmesi aktivizm pratiğini de dönüştürmüş, aktivizmin reel mecralardan dijital mecralara taşınmasına ve bu sayede herhangi bir konu ile ilgili olarak daha fazla kitleye eşzamanlı olarak etkili bir biçimde ulaşmaya olanak tanımıştır. Dijital aktivizmden bahsetmeden önce ona olanak tanıyan dijital dil ile iletişim teknolojilerinin söz konusu dili nasıl kullandığının tartışılması yerinde olacaktır. Dijital dil aslında 19. yüzyılda Matematikçi Wilhelm'in 0 ve 1 değerlerinden meydana gelen aritmetik sistemi bulması ile birlikte ortaya çıkmıştır. Her harf ve sembolün bir kodunun olduğu ve tüm işlerin bu kodlamalar ile yapıldığı dijital dilden, bugün başta bilgisayarlar olmak üzere çok sayıda yeni teknoloji ürünü yararlanmaktadır. Yıllar içerisinde gelişen dijital dil şüphesiz ki yeni iletişim teknolojileri için de büyük önem arz etmiştir. Çünkü dijital dil ile yapılan kodlamayla statik ya da hareketli bir görüntü ve ses kapsayan bir bilgiye ait parça ifade edilebilmekte, bugün tüm dünyada iletişim teknolojileri kapsamında birçok avantaja sahip olan dijital dil analog sistemlere yeğlenmektedir (İspir, 2013: 5).

Dijital dilin ortaya çıkması ve gelişmesinden farklı olarak genel anlamda iletişim teknolojilerinin otuz küsur yıldır içerisinde bulunduğu değişim, dönüşüm ve belki de bu değişimin ortaya çıkardığı en önemli şey olan yeni medya ve internet kavramları da dijital aktivizmin lokasyonel ve düşünsel değişimine etken olmuştur. Froomkin iletişim teknolojilerinin gelişimine paralel yeni medya içerisinde popülerite kazanan internetin diğer sistemlerden kamusal alanlarda gücü çizdiğine, internetin birçok toplumsal pratiği dönüştürdüğüne ve internet tabanlı söylemlerin iletişimsel gücü oluşturduğuna çekmektedir (Froomkin, 2004'den akt. Samuel, 2004: 202). Çünkü bugün birçok toplumsal ya da bireysel pratik internet sayesinde insanların oturdukları yerden yapılabilmekte, dijital sistemler interneti bir eylem ya da pratiğin iletişim ve koordinasyon süreci içerisinde çok güçlü bir araç olarak sunmaktadır. Ayrıca herhangi bir konu ile ilgili şeyler coğrafi sınır göz edilmeksizin internet aracılığı ile milyonlarla takipçilerle ve üyelerle paylaşılabilen, sosyal paylaşım siteleri ile birey kamusal bir alanda kendini temsil edebilmekte, bir konu ile ilgili olarak kitleler internet vasıtası ile kolaylıkla ve hızla örgütlenebilmekte, sosyal ağlar üzerinden yurttaş gündemi belirlemeye teşvik edilmekte ve hatta sosyal mecralar ile dış politika ile ilgili bazı durumlar bile şekillenebilmektedir (Denning, 2000: 242-243).

Aktivizmin dijital mecralara taşınması sonucunda bir kavram olarak ortaya çıkan dijital aktivizm de internete temelli bir pratik olarak ortaya çıkmıştır. Bilgisayar başından herhangi bir konu ya da durum ile ilgili kitleleri örgütlemeyi ifade eden "kliktivizm", bir eylem ya da çağrıya oturduğu yerden, bilgisayar başından bir kaç tık ile destek olmayı ifade eden "slaktivizm" ve politik bazı sebepler görerek hacking işlemi yapmak olan ifade edilen "hacktivizm" gibi türleri ile kendini gösteren ve yeni bir kavram olarak gündeme yerleşen dijital aktivizm internet üzerinden hızla, kitlesel ve eşzamanlı olmakla birlikte diyalojik de bir sürece işaret ettiğinden çok kısa sürede sonuçlar elde edebilmekte, yurttaşlar ve hükümetler için demokratik bir katılıma da işaret etmektedir. Kaplan'a göre (2013), "dijital aktivizm" isminden tam olarak 2010 yılının sonuna doğru gerçekleşen ve ABD Dışişleri Bakanlığı ile konsoloslukları arasındaki yazışmaların deşifre edilmesi olayı ile bahsettirmiş, söz konusu olayı internet ve sosyal medyanın etkisi ve söz konusu mecralardan aldıkları destekler ile gerçekleşen ve hızla yayılan Arap Baharı, Yunanistan ve İspanya'daki olaylar vb. olaylar takip etmiştir. Bu sayede yeni olan iletişim olgusu ile birlikte yeni aktivizm biçimlerinden de bahsedilir olmuştur. Nisan 2009'da gerçekleşen ve Moldova'da çok sayıda gencin, Twitter, Facebook, Bloglar ve Mobil Uygulamalar sayesinde örgütlenip başkentte hükümet aleyhinde protestolarda bulunmaları da önemli bir dijital aktivizm örneği olarak karşımızda durmaktadır (Kök ve Tekerek, 2012: 62).

Uçkan'a göre ise (2012), dijital aktivizm kavram olarak yeni telaffuz edilse de aslında geçmiş olarak eskiye, 1960'lı yılların sonuna dayanan bir geçmişe sahiptir. ARPANET döneminde yani 60'ların sonunda ARPANET'i geliştirmek adına çalışan bilim insanları ile öğrencilerin elektronik posta grupları kurmaları ile

başlayan süreç, söz konusu yerlerde bilim-kurgu ve politika gibi konuların tartışılması ile hem müzakereci bir alan olarak hem de ağ teknolojileri destekli çoksesli bir pratik olarak kendini göstermiş ve aslında bireyler bu alanlarda örgütlenerek ilk dijital aktivizm pratiklerini de gerçekleştirmiştir. Zaten söz konusu dönem ile faaliyetler sonrasında da “internet” denen fenomen doğmuştur. Uçkan dijital aktivizmin toplumsal olarak bir tepki ya da destek faaliyeti olarak iki biçimde kendisini gösterdiğini ifade etmektedir. İlki internet üzerinden ve sıklıkla sosyal paylaşım siteleri üzerinden bir konu ile ilgili örgütlenmek biçiminde seyretmek, diğeri ise internet ile ilgili olumsuz olarak yorumlanan bir durum ya da düzenlemeye tepki göstermek için bloglar ile internet sitelerinin bir mesaj yayınlamak sureti ile kısa bir süre için dahi olsa ekranlarını karartmaları şeklinde seyretmektedir. Bu şekilde düşünsel ya da faaliyetssel olan tepki de dijital bir biçimde gösterilmektedir.

Uçkan’a göre, (2013: 54) temelini internetten aldığını düşündüğümüz dijital aktivizm, internet ve aktivizm arasındaki ilişkiyi açıklayan tek durum değildir ve söz konusu ilişkinin sadece bir bölümünü refet etmektedir. Çünkü artık neredeyse tüm aktivizm türleri interneti kullanmaktadır. Uçkan’a göre, (2013) belki de bu sebep yüzünden ileride “dijital aktivizm” kavramı aktivizmin genel manada dijital bir boyutu kapsayacağı varsayımına paralel kullanılmayacaktır. (Uçkan, 2013) Dijital aktivizmin bir türü olarak bahsedilen hacktivism gibi kavramlar da belki ileride reel faaliyetlerin yerini alan pratiklere dönüşecektir.

2. Bir Dijital Aktivizm Türü: Hacktivism

“Hacktivism” (Hacktivism) kelime olarak “hacking” (hackleme) and “activism” (aktivizm) sözcüklerinin birleşiminden doğmuştur. Hacktivism, hedeflenen bir internet sitesine yönelik ciddi hasarlara neden olmayı hedeflemeyen ama tepki ve rahatsızlığı ifade etmeyi amaçlayan faaliyetlerini kapsar. Örneğin; web hack, e-posta bombardımanı ve virüs gönderimi bazı hacktivist faaliyetlerdir (Denning, 2000: 241). Siber ağlar üzerinden belirli bir amaç doğrultusunda tepki göstermeyi hedefleyen hacktivism en net tanımı ile politik bazı gerekçeler göstermek sureti ile hackleme faaliyetinde bulunmak demektir ve siber bir suç olarak da tanımlanabilmektedir. Çünkü bazı hacktivism faaliyetleri sadece huzursuzluk verecek nitelikte görece “naif” olsalar da (çok sayıda eposta gönderme vs.), bazıları siber suçlar kapsamında ele alınmaktadır (Kelly, 2012: 1672).

Aslında hacking etkinliği internet temelinde oluşmuş olan ağ kültürünün tartışmalı, tehlikeli ve “yanlış” olarak ifade edilen yönlerinden birini oluşturmaktadır. Başlangıçta hacking kelime ve faaliyetler anlamında “yaratıcı ve yenilikçi biçimde bilgisayar programlama” şeklinde ortaya çıkmış ama zamanla politik bir tepki aracına dönüşmüş, hackerlar korsan ifadesi ile bir korku unsuru şeklinde sunulmuştur. Bugün sibertoplumlar ile ağlar için bir tehdit olarak adlandırılmış olan ve “uğursuz” olarak da anılan hackerlar, çevrimiçi protestoları kolaylaştırmak, sivil itaatsizlik yapmak ve küresel sermayeye ağlar üzerinden müdahale etmek noktasında önce çıkmakta ve git gide popülerleşmektedir Ayrıca hacktivismde küresel bilgi akışı ile bilgisayar teknolojisinin yaratıcı kullanımına yapılan büyük vurgu da hacktivismin küresel direnişine de işaret etmektedir (Gunkel, 2005: 575). Hampson’a göre, (2012: 515) internetin gelişmesi ile yaygınlaşan hacktivism aslında hükümet, sıradan yurttaş ve toplumun hemen her bireyinin tartışmalarını ifade etmeye başlamış ve hacktivism ile tepki ya da destek kavramlarını doğrudan ilgilendiren yeni, dijital bir mecra açılmış olmuştur. Busch ve Palmas’a göre, (2006: 29) hacking yani hackleme eylemi önceleri bilgisayarlardaki bekleme sürelerini kısaltmak amaçlı kod kullanımı şeklinde ortaya çıkmış, yıllar içerisinde hackingin eylemsel ruhu yakalanarak önceleri meraklı bilgisayar kurtları tarafından hobi olarak bilgisayarlara sızma, daha sonrasında ise bir tepki biçimine dönüşmüştür

Taylor’a göre (1999), hacktivism 1990’ların aleni bir siyasal duruşudur ve metalaşmış bazı siyasi değer ve uygulamalara karşı bir tepki niteliğindedir. Yamich ve Smith’e göre de, (2012) hacktivism yapan hacktivistler kötü niyetli bir bilgisayar korsanı gibi yıkıcı eylemlerde bulunmazlar, onların hedefleri toplumsal veya siyasi mesajlar iletecek olan bir davaya dikkat çekmektir ve bu genellikle şirket ya da hükümet politikalarına karşı

saldırıları kapsayan misillemeler şeklinde yapılır. Hactivizm politik gerekçelere dayanır çünkü hükümet, kurum ve şahısları bilgi güvenliği ile ilgili düşünmeye zorlar. Kullanıcıları bilgilerin korunması konusunda güvenliğe davet eden hacktivism, internet üzerinde olan ve yayılan bilgiler konusundaki sorumluluğa da dikkat çeler. Buna ek olarak, hacktivism aynı zamanda insanları önemli sosyal ya da siyasi nedenler konusunda destek ya da tepki hususunda düşünmeye zorlar.

Hactivizm çevrimiçi bir sivil müzakere vizyonu sunarak internetin siyaset üzerindeki etkisine dikkat çekerken, tepkisel olan eylem ve uygulamaları ile müzakereci demokrasiyi de çerçeveler aslında (Samuel, 2004: 200).

Hactivist tepkiler ve destekler iki biçimde yürütülmektedir. “Siber ataklar” yani bilgisayar ağları üzerinden bir sistemi çökertmek ya da ele geçirmek yolu ile bir durum ya da kurum ile uygulamaları hacktivistlerce protesto edilebilmektedir. Geleneksel protestolar ile karşılaştırıldığında genellikle bilgisayar ekranı arkasından çeşitli dijital araçlar ile gerçekleştirilen hacktivismin ciddi bir teknoloji bilgisi ve hakimiyeti gerektirdiği söylenebilmektedir. Geleneksel protestolar yürüyüş, eylem ve gösteri vs formatında iken, hacktivism ile söz konusu pratikler biçim değiştirerek dijitalleşirler (Li, 2013: 309).

Hactivizm politik gerekçeler sunmak kaydı ile demokratik bir katılım Houghton’a göre, (2010: 100-101) “Hacking”, “Hacktivism” ve “Cyberterrorism” kavramları ve söz konusu kavramlara ilişkin tartışmalar “İkiz Kuleler” ve Amerika’yı hedef alan diğer terörist saldırıların ardından daha da artmıştır. 9/11 sonrasında, çeşitli yazarlar söz konusu olayları Hacktivism üzerinden ele almışlardır ve 9/11 bağlamında hacktivism ilk tartışma olma onuruna sahip olmuştur. Samuel’e göre (2004) hacktivism ve geleneksel anlamdaki hacking yani hackleme aslında aynı şey değildir ve zaten hacktivism yapan kişileri ifade eden “hacktivist” ile “hacker” da kavram olarak aynı şey değildir, çünkü hacktivist hackerlığın bir türüdür. Hacktivism ile bazen siberterörist atakları, durumları refer eden hacking, temelde toplam üç fark ile birbirlerinden ayrılmaktadır. İlk ayrım hacktivismin şiddetsiz olması, siber terörist atakların ise insanlara zarar verebilecek nitelikte olmasıdır. İkinci ayrım ise, siber terörist atakların genellikle yasa dışı olması, hacktivismin ise genellikle yasal, sadece bazı zamanlar yasadışı faaliyetleri kapsamasıdır. Üçüncü ayrım ise hacktivismin şiddetsiz olmasında dijital araçların kullanılmasıdır. Bu durumda hacktivism siyasi açıdan yalnızca dijital araçları kullanan doğal ve doğrudan suç olmayan bir faaliyet olarak tanımlanabilir. Bununla birlikte hacktivism temelde üç (3) biçimde yapılır. Bunlar; Politik Çatlatma/Parçalama”, “Performatif Hacktivism” ve “Politik Kodlama”dır. Bir hacktivism biçimi olarak Politik Çatlatma/Parçalama hackerlar tarafından yapılan ve yasal olmayan faaliyetleri kapsarken, Performatif Hacktivism politik parçalamadan farklıdır. Çünkü performatif hacktivismin faaliyetleri hacktivistler ve sanatçı kökenli aktivistlerin yasal olduğunu düşündükleri iddialardan oluşur ve genelde politik bir alan baz alınarak politik amaçlar güdülür. Samuel’in açıkladığı şekilde (2004) Politik Kodlamada ise, hackerlar teknik becerilerini saldırgan politikalara dönüştürürler (Samuel, 2004 ve Chan, t.y: 1). Politik kodlayıcılar genellikle özgürlük üzerine vurgu yaparken, internete özgür konuşma alanı anlamı yüklerler (Samuel, 2004: 207).

Politik ve dijital bir tepki biçimi olan hactivizm bünyesinde hackerları ve hacktivistleri olumsuz faaliyetlerden sakındırmak için bazı etik kodlar da bulundurmaktadır. Çünkü hacktivism sadece tepkisel bir anlamda kötü niyet olmadan gerçekleştirildiğinde beraberinde olumsuz sonuçlar getirmezken, hackingin, hacklemenin kötüye kullanılması ile telafisi mümkün olmayan sonuçlar doğabilmektedir. 1984 yılında öncü bir teknoloji gazetecisi olan Steven Levy, hackerların protestolarında benimsedikleri ilkeleri ifade etmek amacı ile “hacker etiği” terimine işaret etmiştir. Toplamda yedi (7) etik ilkeyi benimseyen “hacker etiği” şeklindeki ilkeleri şöyledir:

1. Bilgisayarlara erişim tamamen sınırsız olmalıdır.
2. Hackerlar bireysel emek ve faaliyetleri takdir etmelidir.

3. Enformasyon özgür olmalıdır.
4. Hackerlar yetkililere güvenmemeli ve merkezsizleştirmeye teşvik etmelidir.
5. Hackerlar akranlarını eğitim ya da meslek cinsine göre değil, sadece onların hacking faaliyetleri ile ilgili olarak yargılamalıdır.
6. Bir bilgisayarın sınırları içerisinde güzellik ve sanat yaratmak mümkündür.
7. Bilgisayarlar insan hayatı için daha iyi olabilir (Kelly, 2012: 1676).

Buna karşın aktivistler, insan hakları savunucuları ve Birleşmiş Milletler ve Avrupa İnsan Hakları Mahkemesi tarafından da kabul gören 1950'lerdeki "Hacker Etiği" ise aşağıdaki gibidir:

1. Bilgisayarlara giriş hakkı herkese açık olmalıdır.
2. Bilgi özgür olmalıdır.
3. Otoriteye asla güvenilmemelidir.
4. Hackerlar, hackleriyle değerlendirilmeli ve ölçülmelidir.
5. Hacker, bir bilgisayar aracılığı ile sanat ve güzellik yaratılabileceğini görebilmelidir.
6. Bilgisayarlar hayatı daha iyi yapabileceği gibi, daha kötü de yapabilir (Uçkan, 2013).

Görüldüğü üzere hackerlık ya da hacktivistlik dünyaya ve insanlara faydalı gerekçeler ile gerçekleştirildiğinde kötü bir faaliyete değil, dijital bir aktivizme işaret etmekte ve tepki ya da desteklerin etkisini anında göstererek çabucak sonuç verebilmesine kadar bir yol izlemektedir.

3. Kavram Olarak "Hacker" ve Hacktivist

Hacking eylemi gerçekleştiren kimseler olan "hacker"lar, bilişim sistemlerini hedef alarak çeşitli amaçlar doğrultusunda bir konu ile ilgili siber zarar, tepki ya da destek veren kimseleri ifade etmektedir (Jordan ve Taylor, 2004: 164). Oysaki kelime olarak hacking yarıp çıkarmak, içine bakmak anlamına gelmektedir (Uçkan, 2013). Yani aslında hacking sorunlu olduğu düşünülen bir durum ile olaya dijital bir tepki göstererek onu parçalamak, kırmak, ve yarak içinde olanı çıkarmak adına yapılan eylemlere işaret etmektedir.

Hackerler topluluk içerisinde değil evde bilgisayar başında kendilerini siber kodlarla ile bazı şeylerden soyutlama ve tepki gösterme biçimleri ile ifade ederler ve kavram olarak hacktivistlerden ayrılırlar. Çünkü hacktivistler hackerlardan farklı olarak genellikle siyasi gerekçeler ile hareket ederler. Oysa hackerların bu anlamda bir kısıtlaması yoktur. Sabancı (2013: 17), hacktivistmden farklı olan hacking ve hackerların bir kültür olabileceğini ifade etmektedir. Çünkü bir şeyin kültür olabilmesi onun diğer kültürler ile ilişkisi ile söz konusu kültürlerden ne oranda faydalandığına bağlıdır. Bu bakımdan bakıldığında hackerların benimsedikleri temel etik kodları, bakış açıları, yaşam biçimleri olduğundan ve söz konusu şeyler zaman zaman farklılaşsa da aslında bir kültüre işaret etmektedir. Ayrıca hacking çokselsli yapısı ve kendine özgü unsurları ile salt kültür olarak değil, "karşı bir kültür" olarak da tanımlanabilir (Sabancı, 2013: 17).

Bugün hacker ya da hacktivist deyince bilişim sistemlerini hedef alan, "bilgisayar korsanları" ifadesi ile görece tehlikeli bir kimliğe işaret edilmektedir ve hacktivistler ile hackerlar temelde birbirlerin farksız sanılmaktadır. Oysaki hacktivistler hackerların biri alt biçimdir ve hackerlar kendi içlerinde siber saldırı ve amaçları doğrultusunda yedi (7) türe ayrılmaktadır. Bunlar; Beyaz Şapkalı Hackerlar, Siyah Şapkalı Hackerlar, Script Kiddie, Hacktivistler, Devlet Destekli Hackerlar, Ajan Hackerlar ve Siber Teröristlerdir. Beyaz Şapkalı Hackerlar, güvenlik uzmanları sıfatı ile firmalarda çalışan, sistemlere yönelik kötü niyetli faaliyetler ile olası güvenlik açıklarını tespit ederek bildiren kimselerdir. Siyah Şapkalı Hackerlar, bilişim sistemlerindeki açıkları bularak söz konusu sistemlere sızan, sistemin çalışırılığına zarar veren ve gizli bilgi ele geçiren kimseler iken, Script Kiddielar ise genellikle sistem ve kişilere saldırarak, hasar vermek ya da ele geçirdikleri bilgileri kötü amaçlar doğrultusunda kullanmayı hedefleyen kimselerdir. Bu tip hackerlar teknik açıdan çok donanımlı

değildir, bir program bulurlar ve söz konusu programın yönlendirmeleri ile faaliyetlerini yaparlar. Hacktivistler ise gündemdeki siyasi ve politik olaylar konusundaki tepkilerinin dijital sistemler aracılığı ile gösteren örneğin Türkiye’den RedHack gibi kimselerdir ve herhangi bir bilişim sistemine girerek hem sisteme kendi görüş ve düşüncelerini yazarlar, hem de sistemi çökerterek çalışmamasını sağlarlar. Devlet Destekli Hackerlar, ülkenin bilişim sistemlerini gözeden ve lüzum görüldüğünde ülke ve devletin çıkarları gereği başka sistemlere sızan kimselerdir. Ajan Hackerlar ise rakip şirketlerin gizli bilgi ve ticari sırlarını ele geçirmek için firmalar tarafından para karşılığında tutulan kimselerdir ve son yıllarda bu tip hackerlık ciddi bir artış göstermiştir. Son hackerlık türü olan Siber Teröristler de politik açıdan kendilerini motive ederek, bilişim sistemlerine saldırılar yapan ve bu eylemleri ile toplumların gözünde korkuya sebep olmayı hedefleyen kimselerdir (Turak, 2014: 6).

4. Türkiye’de Hacktivism ve “RedHack”

Hacktivism iletişim teknolojilerinin gelişmesine paralel şekilde dijital aktivizmin bir biçimi olarak kendisinden dünyada “Anonymous”, “Cyber-Warriors”, “LulzSEC”, “The Jester”, “Milw0rm”, “Telecomix” ve “Electronic Disturbance Theater” gibi hacktivist oluşumlar ile söz ettirirken, Türkiye’de ise adından “RedHack” isimli hacktivist oluşum ile söz ettirmiştir (Turak, 2014: 9-10). Hacktivism hem kavram hem de pratik uygulama olarak Türkiye için henüz yeni olsa da, RedHack sayesinde Türk hacktivismi kendisinden dünyada da söz ettirmiştir. Çünkü RedHack eylemlerini toplum ile özgürlük ve bilgiye erişim haklarını göz ederek genellikle politik gerekçeler ile yapmakta, bu anlamda da hackerlık biçimlerinden hacktivismi gerçekleştirme bağlamında Türkiye’de öne çıkmaktadır. Yani RedHack bu varsayımlar doğrultusunda hacktivist bir oluşum olarak tanımlanabilmektedir. “Baskı Altındakilerin Sesi, İnsanlık İçin Adalet!” sloganı ile yola çıkan ve “Gerçekler ile sessizlikler yer değişirse o zaman sessizlikler yalan olur!”, “Sansür Suçtur.”³ gibi ilkeleri savunan “RedHack” yani Kızıl Hackerlar, Kızıl Hackerlar Birliği bir hacker grubu olarak 1997 yılında kurulmuştur ve kendisini “Marksist” ve “Sosyalist” olarak tanımlamaktadır. Türkiye’de 2012 yılının Şubat ayında Ankara Emniyet Müdürlüğü’nün internet sitesini düzenledikleri saldırı ile adından söz ettiren Redhack’in temel kadrosu ise 12 üyeden oluşmaktadır. Atılım Gazetesi’ne 2006 yılında verdikleri bir röportajda görevini “Türkiye ve Kürdistan devrimine hizmet etmek” şeklinde belirten RedHack⁴, yurttaşları Türkiye’de geçtiğimiz aylarda gündemde uzun süre tartışılan internet yasası ile ilgili bilginin özgürlüğü temalı çeşitli şehirlerde eyleme çağırmıştır. Redhack’in çok kalabalık olmayan internet sitesinde eylemleri ile sivil direniş konusunda Türkiye’de meydana gelen eylem ve olaylara ilişkin çeşitli bilgi, video, fotoğraf ve yorum hem İngilizce hem de Türkçe olarak yayınlanmaktadır. Sosyal medya aracılığı ile gelişen vatandaş haberciliğinin ve vatandaşın haber ile bilgiye özgürce erişebilmesi gerektiğinin üzerinde duran ve kendisi de sosyal medyayı da aktif biçimde kullanan RedHack’in resmi Twitter hesabı <https://twitter.com/TheRedHack> adresi iledir.⁵ RedHack Twitter hesabı üzerinden sivil direniş, siyasi karşıt noktasındaki görüşleri ile birlikte eylemlerini de duyurmaktadır. Ayrıca Facebook’da RedHack ismi ile açılmış birçok profil ile birlikte RedHack sempatizanı kimselerin açmış olduğu topluluklar da mevcuttur.

Kimlikleri ve nerede yaşadıkları net olarak bilinmeyen hacktivist oluşum RedHack’in “MaNYaK” nickini kullanan ve Redhack’in lideri olduğu söylenen kimse Radikal Gazetesi’ne verdiği röportajda Türkiye’de yaşadıklarını ve hiçbir örgüt ile bağlantılı olmadıklarını söylemiştir. Redhack’in lideri arkalarında her kesimden insanın, *Aleviler, Atatürkçüler, Ateistler, Kürtler, Lazlar ile Müslümanların* da olduğunu ifade etmiş, örgütlerden çok kimin haklı olduğu ile ilgilendiklerini söyleyen ManNYaK, var oluş nedenlerini “devrimci dayanışma ve devrimin propagandasının bu alanda yapılması” olarak açıklamıştır.⁶

³ Erişim, www.redhack.tumblr.com, 19.06.2014.

⁴ Erişim, <http://tr.wikipedia.org/wiki/RedHack>, 24.06.2014.

⁵ Erişim, <https://twitter.com/TheRedHack>, Erişim Tarihi: 27.06.2014.

⁶ Erişim, http://www.radikal.com.tr/turkiye/redhackin_lideri_sirin_baba_cikti-1086105, 25.05.2014.

2012 yılından bu yana hacktivist faaliyetleri ile Türkiye’de bilişim ve haber özgürlüğüne vurgu yapan RedHack’in siber saldırı yolu ile yaptığı eylemleri ise kronolojik olarak şu şekildedir:

1. 2012 yılı Şubat 27’de RedHack tarafından Ankara Emniyet Müdürlüğü’nün internet sitesinin çökertilmiş ve fazlaca ihbar ile iç yazışma internet üzerinden yayınlanmıştır.
2. RedHack tarafından 20 Nisan 2012 tarihinde İçişleri Bakanlığı sitesine ait olan bir alt sayfaya mesaj bırakılmıştır.
3. RedHack’in saldırısı ile 27 Nisan 2012’de TNet’in internet hizmeti yaklaşık iki saat aksatılmıştır.
4. Mayıs 2012 tarihinde Kara Kuvvetleri Komutanlığı’nın sistemine sızılarak bazı TSK personellerinin bilgileri ifşa edilmiştir.
5. Milli Eğitim Bakanlığı’nın okullara süt dağıtma projesinin gerçekleştiği ilk günde birçok öğrencinin zehirlenmesine tepki göstermek amacıyla 3 Mayıs 2012 tarihinde üç süt firması aynı gün hacklenmiştir.
6. Anneler Günü kapsamında Kadına yönelik şiddete dikkat çekmek için 14 Mayıs 2012’de Aile ve Sosyal Politikalar Bakanlığı’nın internet sitesi hacklenmiş, ana sayfasına bir bildiri koyulmuştur.
7. 29 Mayıs 2012 tarihinde Türk Hava Yolları’nın internet sitesine girilmiş ve greve destek vermek adına bir siber saldırı yapılmıştır.
8. 3 Temmuz 2012 tarihinde Dışişleri Bakanlığı’nın dosya paylaşım sitesine bir saldırı düzenlenmiş, Türkiye’deki çok sayıda yabancı diplomatın kimlik bilgileri Dropbox üzerinden yayınlanmıştır.
9. 16 Temmuz 2012 günü ise protestolarını destekleyen akademisyen ve gazetecilerin tehdit edilmesi gerekçesiyle Ankara Emniyet Müdürlüğü’nün internet sitesinden önceden ele geçirmiş buldukları 77 megabyte boyutundaki ihbarların dosyası olan txt’in tamamı yayınlanmıştır.
10. Diyanet İşleri Başkanlığı’nın ana sayfası 29 Ekim 2012’de hacklenmiş ve hükümete ile Gülen cemaatini hedef alan eleştiriler yayınlanmıştır.
11. 2 Kasım 2012 günü Kamu İhale Kurumu’na saldırılmış ve Adalet ve Kalkınma Partisi’ni 1 kuruşa ihaleye çıkarma şeklinde bir eylem gerçekleştirilmiştir.
12. Maliye Bakanlığı sitesi 7 Aralık 2012 tarihinde hacklenmiş ve memura "temsili olarak" zam verilme eylemi gerçekleştirilmiştir.
13. 5 Aralık 2012’de pedofili yakalatma ve hesaplarını kapatma eylemi gerçekleştirilmiştir.
14. Yüksek Öğretim Kurumu’nun sitesi de 8 Ocak 2013’de ikinci defa hacklenmiş ve ulaşılan yolsuzluk belgeleri yayınlanmıştır.
15. Ankara Büyükşehir Belediye Başkanı Melih Gökçek hakkında 26 Şubat 2013’de bazı belgeler yayınlanmıştır.
16. 22 Mart 2013’de Ankara Büyükşehir Belediyesi internet sitesi hacklenmiştir.
17. MOSSAD’ın internet sitesi Anonymous işbirliği ile 23 Mart 2013’de çökertilmiştir.
18. 24 Mart 2013’de ise üst düzey bürokratlar ve hâkimlerin de aralarında olduğu 32.000 İsrail çalışanının isim, ev ve e-mail adresleri ile diğer kimlik bilgileri deşifre edilmiştir.
19. İstanbul Valiliği’nin 1 Mayıs gösterilerinin Taksim’de yapılmasına onay vermemesi ve göstericilere müdahalesi gerekçesi ile 5 Mayıs 2013 günü İstanbul Valiliği’nin resmi internet sitesi hacklenmiş ve ana sayfaya İstanbul Valisi Hüseyin Avni Mutlu’yu muhatap alan bir protesto notu koyulmuştur.
20. Hatay’ın Reyhanlı ilçesinde 11 Mayıs 2013’de meydana gelen patlama sonrasında ulusal yas ilan edilmesi talep edilerek Hatay Valiliği internet sitesi çökertilmiştir.
21. 22 Mayıs 2013’de Reyhanlı Patlaması ile ilgili Askeri İstihbarat Belgeleri yayınlanmıştır.
22. AB Bakanı Egemen Bağış’ın bazı e-mail yazışmaları 26 Mayıs 2013’de yayınlanmıştır.
23. 30 Mayıs 2013 günü Gezi Parkı yıkımını protesto etmek için İstanbul Beyoğlu İlçe Emniyet Müdürlüğü’nün internet web sitesi hacklenmiştir.
24. 31 Mayıs 2013’de de yine Gezi Parkı yıkımını protesto etmek adına "Hak yersen hack yersin" mottosuyla Gaziantep Büyükşehir Belediyesi’nin internet sitesi hacklenmiştir.
25. Gezi Parkı eylemlerinde vekillerinin ilgisizliği gerekçesi ile kendileri ile eşlerinin cep ile ev telefon numaraları 1 Haziran 2013’de yayınlanmıştır.

26. 8 Haziran 2013 günü Gezi Parkı eylemlerinde polis sert bir tutum göstermiştir gerekçesi ile İstanbul ili emniyet müdürlerinin cep telefon numaraları yayınlanmıştır.
27. Bazı iş adamları ile Tarım Bakanı arasında geçen toplantının kaydı 17 Haziran 2013 tarihinde yayınlanmıştır.
28. İstanbul İl Özel İdaresi'nin sayfası 28 Haziran 2013'te hacklenmiş, kullanıcı bilgileri Twitter üzerinden yayınlanmış ve sistemde takipçilerle beraber değişiklikler yapılması yönünde bir eylem gerçekleştirilmiştir.
29. Sivas İl Özel İdaresi'nin sayfası 2 Temmuz 2013 tarihinde Sivas Katliamı'nı hatırlatmak için hacklenmiş ve erişime kapatılmıştır.
30. Diyanet İşleri Başkanlığı sayfası 3 Temmuz 2013 günü hacklenmiş, kullanıcı bilgileri Twitter üzerinden yayınlanmış, sistemde takipçilerle beraber değişiklik yapılması yönünde bir eylem gerçekleştirilmiştir.
31. Adana Büyükşehir Belediyesi Su ve Kanalizasyon İdaresi 14 Ağustos 2013 tarihinde hacklenmiş, kullanıcı bilgileri Twitter üzerinden yayınlanmak suretiyle sistemde takipçilerle beraber değişiklikler yapılması yönünde bir eylem gerçekleştirilmiştir.
32. Türkiye Kamu İşletmeleri Birliği sitesi 14 Ekim 2013 tarihinde hacklenmiş ve sayfaya bayram mesajı bırakılmıştır.
33. Türkiye Büyük Millet Meclisinin (TBMM) internet sitesi hacklenmiştir.⁷

RedHack'in yukarıda sözü edilen eylemleri Türkiye'de hukuki bazı işlemler ile karşılaşmıştır. Örneğin 21 Mart 2012'de Özel Yetkili Ankara Başsavcılığı bazı şehirlerde operasyonlar yaparak çok sayıda kişiyi gözaltına almış, bu kimselerden Redhack üyesi olduğu iddia edilen 17 kişiden 7'si terör suçu dahilinde tutuklanmış ama daha sonrasında Redhack'ten söz konusu kimselerin grup ile ilişkileri olmadığı beyan edilmiştir. RedHack daha sonrasında ise "bölücü silahlı terör örgütü" suçlamasıyla karşılaşmıştır. RedHack üyesi olmaktan tutuklu bulunan 7 kişiden önce 4'ü, sonra da 3'ü serbest bırakılmıştır. Mayıs 2013'de *Terörle Mücadele Yasası ile görevli Ankara Başsavcı Vekilliği, RedHack'in eylemlerinin "şiddet içermediği" gerekçesiyle, görevsizlik kararı vererek dosyayı Bilişim Suçları Soruşturma Bürosu'na göndermiştir.* Aynı ay Reyhanlı patlamasına ilişkin RedHack'in yayınladığı belgelerin sızdırıldığı dakikaların nöbet saatine denk gelmesi nedeniyle Amasya Komutanlığı'nda görevli bir er olan Utku Kali tutuklanmıştır. RedHack üyeliği suçlamalarını kabul etmeyen Kali'ye özgürlük için Change.org gibi mecralarda imza kampanyaları düzenlenmiş, sosyal medya Kali olayına büyük tepki göstermiştir. Tüm bunların ardından Kali suçsuz bulunmuş ve serbest bırakılmıştır.⁸ Bunun yanı sıra bir dönem RedHack'in internet sitesi mahkeme kararıyla ve 5651 sayılı kanun dayanak gösterilerek engellenmiştir. Ayrıca RedHack'in Türkiye'de adını ilk duyurduğu eylem olan Ankara Emniyeti'nin sitemine sızması ve ele geçirdiği bazı belgeleri deşifre etmesinin ardından şifrelerin genellikle 123456 gibi kolay tahmin edilebilecek numaralardan oluştuğu sistemle ilgili Emniyet'ten söz konusu sistemlerin zaten çok da önemli olmadıkları yönünde bir açıklama getirilse de, şifrelerin kolaylığı güvenlik zafiyetini akıllara getirmiştir (Uçkan, 2013 69).

RedHack Ankara Emniyet Müdürlüğü'ne yönelik düzenlediği siber eylemlerinin aslında Ankara Emniyet Müdürlüğü'nün bazı şifrelerinin 123456 şeklinde emniyetsiz olduğu iddia edilen rakamlardan oluşmasına bir uyarı niteliğinde olduğunu da dile getirmiştir.

5. Siber Güvenlik ve Türkiye

Türkiye'de siber güvenlik konusu yakın bir zamanda ele alınmış ve 2004 yılında kabul edilen 5070 sayılı *Elektronik İmza Kanunu ile 2008'de kabul edilen ve haberleşme sektörünü düzenlemeyi amaçlayan Elektronik Haberleşme Güvenliği Yönetmeliği* (Ünver ve Canbay, 2010'dan akt. Hekim ve Başbüyük: 2013: 154) siber alanı biçimlendiren ilk kanunlar olarak karşımızda çıkmaktadır. Ayrıca 2006 yılında *Resmi Gazete'de yayınlanan 2006/38 sayılı Yüksek Planlama Kurulu Kararında yer alan Bilgi Toplumu Stratejisi ve Eki Eylem Planında*

⁷ Erişim, <http://tr.wikipedia.org/wiki/RedHack>, 24.06.2014.

⁸ A.g.i.s.

“Güvenlik ve Kişisel Bilgilerin Mahremiyeti” başlığı dahilinde bilgi güvenliğine dair hukuki düzenlemeler ve bilgisayar olaylarına hemen müdahale merkezinin oluşturulması ile kamu kurumlarının bilişim güvenliğinin yapılmasına yönelik faaliyetlerden bahsedilmiştir. Hemen sonrasında “TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi” kapsamında “Bilgisayar Olaylarına Müdahale Ekibi” kurulmuştur. Daha sonrasında Siber Güvenlik Kurulu’nun kurulması ile siber güvenlik noktasında daha net ve kapsayıcı adımlar atan Türkiye bu kurulun kararı ile Ulaştırma Bakanlığı ulusal siber güvenliğin temini noktasında *politika, strateji ve eylem planlarının hazırlanması* konusunda görevli kılınmıştır. Ayrıca 27 Mayıs 2013 tarihinde Telekomünikasyon İletişim Başkanlığı’nda kurulan ve *Sektörel ve Kurumsal Siber Olaylara Müdahale Ekipleri* ile beraber siber güvenliğin temini kapsamında çalışacak olan “Ulusal Siber Olaylara Müdahale Merkezi” (USOM) da siber güvenlik noktasında ulusal koordinasyon ve uluslararası işbirliği noktasında atılan önemli bir adım olarak karşımızda durmaktadır (Turak, 2014: 14-15).

Bu anlamda önemli bir adım olan siber güvenliğin Türkiye için eski bir geçmişinin bulunmadığını ve siber güvenliğin yalnızca son yıllarda kabul edilen kanun ve bazı yönetmelikler ile çerçevelendiğini de belirtmek gerekmektedir (Hekim ve Başbüyük: 2013: 154).

Sonuç ve Değerlendirme

Aktivizmi iletişim teknolojileri ve internet aracılığı ile dönüştüren ve siber uzama yerleştiren dijital aktivizmin bugün her biçimi ile kendini sosyal yaşamda da gösterdiği açıktır. Bu anlamda dijital aktivizmin bir biçimi olan hacktivism de tüm dünyada olduğu gibi Türkiye’de de yeni bir kavram olarak siber gündeme oturmuştur. Politik gerekçeler ile internet üzerinden siber saldırı, protesto ya da eylem biçiminde yapılan hacktivism bireysel tepkinin siber biçim ile yer değiştirmesini de ifade etmiştir. Bir dijital aktivizm pratiği olan hacktivism RedHack örneği ile ele alan bu çalışma sonunda görülmüştür ki; Türkiye’de son yıllarda eylemleri ile adından söz ettiren RedHack’in 2012 ile 2013 yılları arasında yaptığı yaklaşık 33 siber saldırı ya da protesto politik gerekçeler ile olduğundan RedHack Türkiye’de hacktivist bir oluşum olarak yapılmış durumdadır. Çünkü eylemleri, politik gerekçelere dayanmakla birlikte, bu çalışmada aktarıldığı üzere genellikle enformasyon özgürlüğü ile enformasyonun sahiplik yapısına bir tepki niteliğindedir. RedHack’i kötü niyetli bilgisayar korsanlarından ayıran şey ise RedHack’in hackerlığının bir biçimi olan hacktivismi benimseyen hacktivist bir oluşum olması ile temelde birey yararı gütmesidir. Bununla birlikte bazı eylemlerinden anlaşıldığı üzere RedHack bireyleri cinsiyet, din, dil, ırk, siyasi görüş vs bağlamında ayırt etmemekte, eylemlerini hemen herkesinden bireyin yarar ve haklarını göz ederek yapmaktadır.

RedHack’in Anneler Günü nedeniyle kadına yönelik şiddete dikkat çekmek adına 14 Mayıs 2012’de Aile ve Sosyal Politikalar Bakanlığı’nın internet sitesi hacklemesi ve sitenin ana sayfasına bildiri koyması ile MEB’nin okullara süt dağıtım projesinin gerçekleştiği ilk günde birçok öğrencinin zehirlenmesine tepki göstermek adına 3 Mayıs 2012’de üç süt firmasının aynı gün hacklenmesi RedHack’in bu tutum ve duyarlılığından bazı örneklerdir ve RedHack’in toplumsal sorunlara duyarsız kalamadığının açık birer göstergesidir.

2012 Temmuz’da Dışişleri Bakanlığı’nın internet sitesini hackleyen RedHack hükümet tarafından terör örgütü kategorisine alınmış ve bu durum Uykusuz Dergisi’nin bir karikatürüne de yansımıştır. Karikatür’de “RedHack orak çekiçten oluşan logosundan dolayı terör örgütü kapsamına alındı.” ifadesinin ardından resmedilen kişinin ağzından “Kendi Hacker’lerimizi yetiştirmenin zamanı geldi.” ifadesine “İMAM HACKER LİSESİ” yazılı bir tabela önünde yer verilmiştir. Uykusuz Dergisi’nin bu karikatürü derginin RedHack’e verdiği desteğin örtük bir işareti olarak nitelebilir.⁹ Çünkü RedHack kanımca sosyal ve toplumsal sorunlara dikkat çekmek, internet üzerinden çok sayıda insan ulaşmış ve bazı çevreleri uyararak adına yaptığı siber eylemleri sebebiyle birçok kişinin bir anlamda sempatisini kazanmış durumdadır. RedHack’in 4 Kasım 2014 tarihi itibariyle

⁹ <http://www.gazeteciler.com/karikatur/uykusuzdan-redhack-yorumu-53686h.html>, 03.11.2014.

"https://twitter.com/KizilHackerLAR" adresindeki Twitter hesabında 70.730 takipçiyeye sahip olması ve "https://www.facebook.com/RedHackTaraftar" adresindeki RedHack Sempatizanları isimli oluşumun 195.336 üye bulundurması da bu durumun kısmi bir tespiti niteliğinde görülebilir.

Kasım 2012'de açlık grevlerine destek vermek adına ODTÜ'den Başbakanlık'a kadar yürümek isteyen öğrencilere polisin müdahalesine bir tepki olarak Redhack'in ODTÜ sitesindeki öğrenci dökümanları ile birlikte ODTÜ'nün mail sistemini hacklemesi de RedHack'in hem toplumsal olaylara dikkat çekme çabasına, hem de Türkiye'nin en önemli üniversitelerinden internet sisteminin zafiyetine dikkat çekme gayretine işaret etmektedir. ODTÜ'nün internet trafiğinin merkezi ve sistemlerinin "en güvenilir sistemler olması" gerektiğini belirten RedHack'in söz konusu eylemi tıpkı Ankara Emniyet Müdürlüğü sisteminin güvenlik zafiyeti iddialarına yapılan uyarı gibi bir uyarı niteliğindedir.¹⁰ Bu anlamda RedHack'in yalnızca sosyal bazı olaylara dikkat çekme çabasında olmadığı, bu çabanın yanı sıra Türkiye'deki bazı kurum ve kuruluşları siber güvenlik konusunda daha temkinli olmaya davet ettiği de düşünülebilir. Ayrıca Mart 2012'de KESK üyelerine yönelik "şiddeti" protesto etmek adına Emniyet'e ait 350 internet sitesini kullanılmaz hale getiren RedHack'in söz konusu eylemi 30 Mart 1972 tarihinde özgür bir dünya kurmak için mücadele verdiğini ve katledildiğini söyledikleri Mahir Çayan'a ithaf ettiğini söylemesi de bu noktada önemlidir.¹¹

RedHack'in görüldüğü üzere toplumsal olaylar noktasında yaşananlara kayıtsız kalmadığı açıktır. Bu anlamda okullara süt dağıtımı sonrasında yaşanan zehirlenme vakalarına (ki Milli Eğitim Bakanı Ömer Dinçer, "olayın zehirlenme vakası değil, çocukların süte karşı hassasiyetinden kaynaklanan bir durum" olduğunu söylemesine karşın) bir tepki olarak süt firmalarını hacklemesi aslında RedHack'in Twitter'dan yaptığı açıklamaya göre aslında süte hassasiyet gösteren ya da zehirlenen çocuklar üzerinden, Denizli'de 3 yaşındaki çocuğa 20 kişinin tecavüz ettiği yönündeki iddialara da bir tepki ve uyarı niteliğindedir. Bu bağlamda RedHack söz konusu iddiaya dayanan eylemini şu sözlerle ifade etmiştir:

"Tecavuz'ede Sutu Bozuk'larada Sansure'de Cemaat Terorune'de Tiyatro Yikimlarina'da sessiz kalmayacagiz! Her zalim bir gun RedHack'i tadacak!"

Anlaşıyor ki, RedHack söz konusu süt firmalarının internet sitelerini hackleyerek hem okullarda dağıtılan süttten zehirlendikleri iddia edilen çocuklara, hem de onlardan farksız olan tecavüz mağduru çocuklara dikkat çekmek ve yetkilileri göreve çağırma hedeflemiştir. Çünkü çocuklar nerede olurlarda olsun küçük ve kendini savunamayacak kimselerdir. Kamuoyunda söz konusu olaylarda sıklıkla mağdurların değil, suçluların korunduğu izlenimi büyük oranda inanılan bir durum olduğundan RedHack, toplumu üzen ama hakkında bir şey yapılmayan ya da yapıp yapılmadığı bilinmeyen olaylara karşı bir tepki olarak siber saldırılar gerçekleştirmektedir.¹² Ayrıca RedHack'in Twitter'da paylaştığı iletisinden sansür, cemaat tartışmaları ve tiyatro yıkımı gibi konular noktasında da tepkili olduğu açıktır.

Sonuç olarak çalışmada ele alınan eylemleri (toplam 33 eylem) ile hacktivist bir oluşum olan RedHack'in hükümet politikalarını hedef aldığı ve temelde enformasyonun bir yurttaş hakkı olduğunu savunduğu gözlenmiştir. Bununla birlikte RedHack'in bu çalışmada bahsedilen eylemleri toplumsal bazı olay ve sorunlara dikkat çekme çabası olarak da yorumlanabilir. Radikal bir değişiklik yaratmasa da, RedHack'in eylemleri içtimai sorunlara ve olaylara kendi tarzlarında dikkat çekmek suretiyle aslında devlet kurumları için bir uyarı niteliğinde olmuş, RedHack'in toplumun hassasiyetlerini görmezden gelmediğine işaret etmiştir. Bunun yanı sıra çalışmada bahsedildiği üzere Türkiye'de yaklaşık 10 yıllık bir geçmişi olan siber olayları düzenleyen

¹⁰ <http://www.ulusalkanal.com.tr/teknoloji/redhack-odtuyu-dize-getirdi-h6648.html>, 03.11.2014.

¹¹ <http://www.odatv.com/n.php?n=redhack-bu-eylemi-hangi-devrimciye-afetti-3003121200>, 04.11.2014.

¹² <http://www.gidahareketi.org/-kabahat-Sutte-Degil-Cocuklarda-ymis-1416-haberi.aspx>, 02.11.2014.

yasalar ile uygulamaların iletişim teknolojileri bağlamında daha geniş bir yelpazede ele alınması gerekmektedir. Çünkü internet denen olgu hemen her gün yeni şeylere gebe kalmakta ve beraberinde iletişim süreci kadar toplumsal pratikler noktasında da birçok değişiklik getirmektedir.

Ayrıca hacktivism ve RedHack, yeni bir kavram ve oluşum olarak Sirkka Minkinen'in ilk kez 1978 yılında tanımladığı, bireyin birçok konuda becerisini artırmayı (İnceoğlu, 2011) ve medya metinlerini anlamlandırmayı (Massey, 2006: 1-23) öngören medya okuryazarlığı bağlamında da iyi analiz edilmelidir. Çünkü hackerlık ya da hacktivism bazen medya ya da çeşitli güç odakları tarafından kötü niyetli bilgisayar korsanlığı şeklinde yansıtılabilmektedir. Bugün birçok insan hacker, hackerlık ya da hatta hacktivism denildiğinde aklına kişisel internet kullanımlarına gelecek kötü niyetli faaliyetler gelebilmektedir.

Kaynakça

- BUSCH, Von Otto & PALMAS, Karl, (2006), "Abstract hacktivism the making of a hacker culture", Published in collaboration with OPENMUTE.org, Lightning Source UK Ltd, United Kingdom.
- CHAN, Terence, (t.y.) "Hacktivism", Erişim: <http://ebookbrowse.net/terence-chan-hacktivism-pdf-d368761290>, 21.07.2014, pg.1-11.
- DENNING, E. Dorothy, (2000), "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," Nautilus Institute. A revised version appeared in *The Computer Security Journal*, Vol. XVI, No. 3, pg. 15-35.
- GUNKEL, J. David, (2005), "Editorial: Introduction to Hacking and Hacktivism", *New Media & Society*, Vol 7 (5), pg. 595-597, Sage Publications.
- HAMPSON, C.N. Noah, (2012), "Hacktivism: A New Breed of Protest in a Networked World", 35 B.C. Int'l & Comp. L. Rev. Pg. 511-542, Erişim, <http://lawdigitalcommons.bc.edu/iclr/vol35/iss2/6>.
- HEKİM, Hakan & BAŞIBÜYÜK, Oğuzhan, (2013), "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", *Uluslararası Güvenlik ve Terörizm Dergisi*, 4 (2), s.135-158.
- HOUGHTON, J. Tessa, (2010), "Hacktivism and Habermas: Online Protest as Neo-Habermasian Counterpublicity", A thesis submitted in partial fulfilment of the requirements for the Degree of Doctor of Philosophy in Media and Communication in the University of Canterbury by University of Canterbury.
- İNCEOĞLU, Yasemin, (2011), "Medyayı Doğru Okumak", (Ed.) Melda Cinman Şimşek & Nurçay Türkoğlu, *Medya Okuryazarlığı içinde*(I. Uluslar arası Medya Okuryazarlığı Konferansı Bildirileri, 23-25 Mayıs 2005), 1. Baskı, Parşömen Yayınları, İstanbul.
- İSPİR, Burçin, (2013), *Dijital İletişim ve Yeni Medya içinde "Yeni İletişim Teknolojilerinin Gelişimi"*, s. 2-25, Ed. Mesude Canan Öztürk, T.C. ANADOLU ÜNİVERSİTESİ YAYINI NO: 2956 AÇIKÖĞRETİM FAKÜLTESİ YAYINI NO: 1911, Eskişehir.
- JORDAN, Tim & TAYLOR, Paul, (2004), *HACTIVISM AND CYBERWARS Rebels with A Cause*, Published by Routledge, London.
- KAPLAN, Tuğba, (2013), "Dijital Aktivist Olmanın Yolları", Erişim; http://www.zaman.com.tr/pazar_dijital-aktivist-olmanin-yollari_2103324.html, 27.05.2014.

- KELLY, B. Brian, (2012), "INVESTING IN A CENTRALIZED CYBERSECURITY INFRASTRUCTURE: WHY "HACKTIVISM" CAN AND SHOULD INFLUENCE CYBERSECURITY REFORM", Boston University Law Review, Vol. 92: 1663, pg.1663-1711.
- KÖK, Selcen & TEKEREK, Mehmet, (2012), SOKAK SİYASETİNDEN SOSYAL AĞLARA YENİ AKTİVİZM: ARAP BAHARI DENEYİMİ, II. BÖLGESEL SORUNLAR ve TÜRKİYE SEMPOZYUMU, s. 59-65.
- Lİ, Xiang, (2013), HACKTIVISM AND THE FIRST AMENDMENT: DRAWING THE LINE BETWEEN CYBER PROTESTS AND CRIME, Harvard Journal of Law & Technology Volume 27, Number 1, pg. 301-330.
- MASSEY, Kimb, (2005), Media Literacy Workbook, Second Edition, Thomson Learning Academic Resource Center, Canada.
- SABANCI, Ahmet, (2013) "Hackerlara bir karşı kültür olarak bakmak", Hack Kültürü ve Hacktivism: Yeni bir Siyaset Biçimi içinde, s. 16-26, Der. Ali Rıza Keleş ve Yetkin Sal, Alternatif Bilişim Derneği, İstanbul.
- SAMUEL, W. Alexandra, (2004), "Hacktivism and the Future of Political Participation", to the Department of Government in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the subject of Political Science Harvard University Cambridge, Massachusetts.
- TAYLOR, Paul (1999) Hackers: Crime in the Digital Sublime, Routledge Publications, London.
- TURAK, Yiğit, (2014), "RedHack Özelinde Siber Olaylar ve Siber Suçlar" T.C İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü ITL505–Türk Hukukunda Bilişim Suçları ve Uygulaması Dersi Projesi, s.1-21, İstanbul.
- UÇKAN, Özgür, (2013) "Dijital Aktivizmin Sınır Boyunda Hacktivism: Anonymous ve RedHack örnekleri...", Hack Kültürü ve Hacktivism: Yeni bir Siyaset Biçimi içinde, s. 53-79, Der. Ali Rıza Keleş ve Yetkin Sal, Alternatif Bilişim Derneği, İstanbul.
- UÇKAN, Özgür, (2012), "Dijital Aktivizm Mi?" "Aktivizm Mi?", Erişim, <http://spotdergi.wordpress.com/2012/05/30/dijital-aktivizm-mi-aktivizm-mi/>, 13.05.2014.
- YAMICH, John & SMITH, Anthony, (2012), "Anonymous and LulzSec: The impact hacktivist organizations have on our perceptions of hackers and information security", Purdue University, Erişim; http://www.itera.org/wordpress/wp-content/uploads/2012/09/ITERA12_Paper06.pdf, 20.07.2014.

Elektronik Kaynaklar:

- <https://twitter.com/TheRedHack>, Erişim Tarihi: 27.06.2014.
- <http://tr.wikipedia.org/wiki/RedHack>, Erişim Tarihi: 24.06.2014.
- <http://redhack.tumblr.com/>, Erişim Tarihi: 19.06.2014.
- http://www.radikal.com.tr/turkiye/redhackin_lideri_sirin_baba_cikti-1086105, Erişim Tarihi: 25.05.2014.